Amendments to the Specification:

Please replace paragraph beginning on page 1, line 6 and ending on page 1, line 28 with the following amended paragraph:

In the totality of features of the claimed method the following terms are used:

- secret key presents a bit combination known only to a legitimate user;

- encryption key is a bit combination used in encrypting data information signals; encryption key is encryption changeable element and is used for converting the given message or the given totality of messages; encryption key is formed according to determined procedures and the secret key; in a number of ciphers, the secret key as such is used;

~~-cipher is a totality of elementary steps of input data conversion using an encryption key; a cipher may be implemented as a computer program or as an individual electronic device;~~-data-dependent operation is an operation depending on some data subblock, for example, data-dependent rotation operation is used in the RC5 cipher [R.Rivest, The RC5 Encryption Algorithm, Springer-Verlag LNCS, v.1008, 1995, pp.86-96];

- subkey is a portion of encryption key used at individual elementary encryption steps;

- ciphering is a process implementing a certain data conversion method using an encryption key translating the data into a cryptogram which is a pseudo-random character sequence from which it is practically impossible to obtain information without knowing the value of the encryption key;

- deciphering is a process which is reverse to ciphering procedure; deciphering ensures recovering information according to the cryptogram when the encryption key is known;

-cryptographic resistance is a measure of safety of information protection and represents labour intensity measured in the number of elementary operations to be performed in order to recover information according to the cryptogram when the conversion algorithm is known but without the knowledge of the encryption key.

Please replace paragraph beginning on page 3, line 7 and ending on page 3, line 12 with the following amended paragraph:

The above task is achieved by the fact that in the method for block encryption of discrete data, including generating an encryption key as a set of subkeys, breaking down the data block into $N\geq 2$ subblocks and ~~alternate subblock conversion~~ converting in turn said subblock by performing a ~~dual locus~~ two-place operation on a subblock and a subkey, the novel feature, according to the invention, is ~~performing j-th subblock-dependent conversion operation, where $j\neq 1$, on the subkey,~~ transforming subkey with the data-dependent operation that depends on the j-th subblock prior to carrying out the ~~dual locus~~ two-place operation on the i-th subblock, where $j\neq i$, and subkey.

Please replace paragraph beginning on page 3, line 18 and ending on page 3, line 19 with the following amended paragraph:

A novel feature is also the fact that ~~as the j-th subblock-dependent conversion operation, a j-th subblock-dependent subkey bit permutation operation is employed.~~ data-dependent permuting subkey bits is used as data-dependent operation that depends on the j-th subblock.

Please replace paragraph beginning on page 3, line 22 and ending on page 3, line 23 with the following amended paragraph:

A novel feature is also that ~~the j-th subblock-dependent subkey bit cyclic offsetting operation is used as a j-th subblock-dependent conversion operation~~ data-dependent rotation of subkey bits is used as data-dependent operation that depends on the j-th subblock.

Please replace paragraph beginning on page 3, line 26 and ending on page 3, line 28 with the following amended paragraph:

Further, the novel feature is that ~~the j-th subblock-dependent permutation operation performed on the subkey is employed as a j-th subblock-dependent conversion operation~~ data-dependent substitution operation performed on subkey is used as data-dependent operation that depends on the j-th subblock.

Please replace paragraph beginning on page 8, line 28 and ending on page 9, line 13 with the following amended paragraph:

This example explains the use of ~~cyclic offsetting operation depending on subblocks being converted and performed on subkeys~~ data-dependent rotation operations for transforming the corresponding subkeys. The encryption key is generated in the form of 16 subkeys K_1, K_2, K_3,..., K_{32}, each having a length of 32 bits. An input 64-bit data block is broken down into two 32-bit subblocks A and B. ~~Encrypting~~ Encryption of the input block is described by the following algorithm:

1. Set round number counter r=1.

2. Convert subblock B according to the expression: B: $=B \oplus (K_{2r}<<<A)$, where $K_{2r}<<<A$ signifies ~~an operation of cyclic offsetting to the left~~ the to-left rotation operation by A bits executed on subkey K_{2r}.

3. Convert subblock A according to the expression:

A: $=A \otimes B$,

where "$\otimes$" is modulo 2^{32} summation operation.

4. Convert subblock A according to the expression:

A: $=A \oplus (K_{2r-1}<<<B)$,

where $K_{2r-1}<<<B$ signifies ~~an operation of cycling offsetting to the left~~ the to-left rotation operation by B bits executed on subkey K_{2r-1}.

5. Convert subblock B according to the expression:

B: $=B \otimes A$.

6. If $r\neq16$, then increment counter r: =r+1 and move to step 2, otherwise STOP.

Please replace paragraph beginning on page 9, line 14 and ending on page 9, line 22 with the following amended paragraph:

The logic pattern of one conversion round is explained in Fig.1, blocks P_1 and P_2 in this example represent an operating block performing ~~an operation of cycling offsetting bits of~~ the data-dependent rotation operation on corresponding subkeys depending of subblocks being converted. This algorithm is oriented to implementing in the form ~~of~~ on a computer program. Modern ~~microprocessor~~ microprocessors quickly carry out the ~~cyclic offsetting~~ rotation operation depending on the value of a variable stored in one of registers. Due to this fact, the described algorithm, when realised in software, provides ~~the~~ an encryption rate of about 40 Mbit/s for a mass-volume microprocessor Pentium/200. When 10 encryption rounds are set, a rate of about 60 Mbit/s is achieved.